NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ
Ara, bul.

Sosyal Bilimler Enstitüsü Dergisi
Cilt: 15 Sayı: 1 Mart 2025
E-ISSN: 2149-3871

SOSYAL MEDYADA SİBER SUÇLAR: ÜNİVERSİTE GENÇLİĞİ ÜZERİNE UYGULAMA

CYBER CRİMES on SOCİAL MEDIA: APPLİCATİON UNİVERSİTY YOUTH

İbrahim AKKAŞ
EBYÜ İ.İ.B.F.Sosyal Hizmet Bölümü
iakkas@erzincan.edu.tr
ORCID: 0009-0006-1381-2982

Geliş Tarihi:
18.01.2025

Kabul Tarihi:
20.03.2025

Yayın Tarihi:
27.03.2025

Anahtar Kelimeler
Sosyal medya,
Suç,
Siber Suç,
İnternet.

Keywords
Social Media,
Crime,
Cyber Crime,
Internet.

ÖZ

Gelişen teknolojik çağda internet, özellikle sosyal medya hayatımızda önemli bir rol oynamaktadır. Çünkü sosyal medya sayesinde herkes yakınları ve sevdikleriyle kolaylıkla iletişim kurabilmektedir. Instagram, Twitter, Facebook, Youtube ve Linkedin gibi kullanıcıların günlük olarak kullandıkları, aileleri, arkadaşları ve akrabaları ile kolayca iletişim kurabildikleri ve verilerini paylaşabildikleri birçok ağ bulunmaktadır. Sosyal medya, internet bağlantılı dünyada yeni iletişim yollarını açmıştır. Bu iletişim, dünyanın her yerindeki insanlar arasında tweet'leri, fotoğraf, resim, beğeni ve yorum vb. paylaşmayı içerir. Geçtiğimiz yıllarda internet kullanım istatistiklerini incelediğimizde çevrimiçi sosyal ağ sitelerinin, Twitter, Facebook, LinkedIn, MySpace, YouTube, Tiktok, whatsapp gibi sosyal medyayı kullanarak kullanıcıların aileleri, arkadaşları, profesyonel grupları ve diğer topluluklarla iletişim kurmaları için önemli rol oynadığını görmekteyiz. Bununla birlikte, sosyal medya siteleri kullanıcılar için çeşitli ciddi güvenlik riskleri ve tehditleri oluşturmaktadır. Siber suçun artan oluşumuyla birlikte sosyal medyanın kullanımı, günümüzün dijital çağında yükseköğretim kurumları için önemli avantajlar ve dezavantajlar sunmaktadır. Bu çalışma, özellikle üniversite öğrencilerinde sosyal medya kullanımı ile siber suç farkındalığını belirlemeyi öngörmektedir. Bu çalışmanın amacı, sosyal medyayı aktif olarak kullanan üniversite öğrencileri arasında sosyal medya kullanım modellerini, siber suçun yaygınlığını ve bu zorlukları ele almak için etkili stratejileri analiz etmektir. Bu araştırma, eğitim kurumlarındaki dijital teknolojilerin gelişen manzarasına dair değerli içgörüler sunarak, etkili müdahaleler ve politika çerçeveleri üzerine gelecekteki araştırmalar için temel oluşturmaktadır. Araştırma sonucunda öğrencilerin sosyal medyada yaşanabilecek siber suçlar hakkında bilgi sahibi olduğu sonucuna ulaşılmıştır.

ABSTRACT

In the developing technological age, the internet, especially social media, plays an important role in our lives. Because thanks to social media, everyone can easily communicate with their relatives and loved ones. There are many networks such as Instagram, Twitter, Facebook, Youtube and Linkedin that users use daily, where they can easily communicate with their families, friends and relatives and share their data. Social media has opened up new ways of communication in the internet-connected world. This communication includes sharing tweets, photos, pictures, likes and comments, etc. between people all over the world. When we examine the internet usage statistics in the past years, we see that online social networking sites play an important role for users to communicate with their families, friends, professional groups and other communities using social media such as Twitter, Facebook, LinkedIn, MySpace, YouTube, Tiktok, WhatsApp. However, social media sites pose various serious security risks and threats for users. With the increasing occurrence of cybercrime, the use of social media offers significant advantages and disadvantages for higher education institutions in today's digital age. This study investigates the use of social media and cybercrime awareness, especially among university students. The purpose of this study is to analyze social media usage patterns among university students who actively use social media, the prevalence of cybercrime, and effective strategies to address these challenges. This research provides valuable insights into the evolving landscape of digital technologies in educational institutions, laying the groundwork for future research on effective interventions and policy frameworks. The study concluded that students are knowledgeable about cybercrimes that can occur on social media.

DOI: https://doi.org/10.30783/nevsosbilen.1622545
Atıf/Cite as: Akkaş, İ. (2025). Sosyal medyada siber suçlar: Üniversite gençliği üzerine uygulama. *Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi, 15*(1), 472-488.

Giriş

Teknolojinin gelişmesine bağlı olarak artık insanların haberleşme şekilleri de değişmiştir. Günümüzde aktif olarak kullanılan sosyal medya iletişim ve sosyalleşmenin bir aracı olmuştur. İnsanlar, sosyal medya platformlarında paylaşımlar yaparak, iletişim kanalları yoluyla hiç tanımadığı insanlara da ulaşabilmektedirler. Sorun burada ortaya çıkmaktadır. Çünkü kişiler kimlik bilgileri dahil olmak üzere birçok kendine ait özel bilgileri bu platform aracılığıyla daha fazla insanın eline ulaşmasına neden olmaktadır. Burada karşımıza yeni bir suç türü çıkmaktadır. Siber suç olarak adlandırılan yeni suç türü özellikle internetin ve sosyal medyanın kullanımın artmasıyla birlikte hız kazanmış ve yeni suçların ortaya çıkmasına sebebiyet vermektedir.

Sosyal medyaya olan ilgi 2000'li yılların başında başlamış ve günümüze kadar geçen sürede popülerliği artarak devam etmiştir. Facebook, YouTube, Twitter, Instagram ve Snapchat gibi sosyal ağlar dünya çapında milyarlarca aktif kullanıcıya sahiptir. Sosyal medya, bilgi ve medyayı paylaşmanın kolaylığı ve belirli ilgi kitlelerine ulaşma ve onlarla etkileşim kurma yeteneği nedeniyle hem kuruluşlar hem de bireyler için paha biçilmez bir araç olmaya devam etmektedir. Devasa kullanıcı tabanı, iletişim kolaylığı ve veri paylaşımı nedeniyle sosyal medya, siber suçların işlenmesi için uygun bir zemin sunmaktadır. Siber suçlular sosyal medya kullanıcılarını aktif olarak hedef alarak siber suç faaliyetlerini kolaylaştırmak için sosyal medyayı kullanmaktadırlar (Umeugo, 2023: 23).

21. yüzyılın ardından dünya, internet kullanımında ve ilgili teknolojilerde benzeri görülmemiş bir genişlemeye tanık olmuştur. Bu artış topluluklara, işletmelere ve bireysel yaşamlara nüfuz ederek iletişim kurma, çalışma ve öğrenme biçimimizi hızlı bir şekilde değiştirmiştir. Küresel olarak alışveriş, bankacılık, eğlence ve hatta sosyalleşme gibi geleneksel etkinlikler hızla çevrimiçi ortama sosyal medyaya taşınmıştır. Ancak internet ve sosyal medya küresel bağlantı ve bilgi paylaşımı için sayısız fırsat sunarken, aynı zamanda yasadışı faaliyetler için de bazı riskleri beraberinde getirmiştir. Bu yeni bulunan dijital ortam, yenilikçi suç yollarının ortaya çıkmasına, yeni suç biçimlerinin yaratılmasına ve geleneksel suçların sanal aleme ustalıkla uyarlanmasına yol açmıştır (Mwiraira vd., 2023: 35).

Gelişen teknolojiye bağlı olarak günümüzde tek bir tıklama ile dünyanın diğer ucunda siber saldırı gerçekleşmektedir. Dolayısıyla siber suçun, elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların kanuni olmayan şekilde değiştirilmesi, silinmesi veya bilginin elde edilmesi için hazırlık yapılması olarak tanımlandığı görülmektedir (Sandilaç, 2022: 142).

Sosyal medya kullanıcılarının sayısının artması nedeniyle siber suçların sayısı, her geçen gün önemli ölçüde artmaktadır. Bu makalede, çeşitli siber suç türlerini açıklayarak sosyal medyadaki siber suçlara genel bir bakış sunulmaktadır. Ardından sosyal medyayı en yaygın kullanan üniversite öğrencilerinin sosyal medyada ortaya çıkabilecek siber suç türleri hakkında bilgi sahibi olup olmadıklarını araştırmaktadır.

Literatür İncelemesi

Sosyal medya, Facebook, LinkedIn, Twitter, Instagram vb. aracılığıyla dünya çapındaki insanlarla bağlantı kurmak ve ağ oluşturmak için kullanılır. Ağ oluşturma, içerik, hikâye, fotoğraf, video mesajı vb. paylaşımı yoluyla farklı sosyal medya platformları aracılığıyla profesyonel ve kişisel bağlantıları içerir (Kaur vd., 2024: 1).

Sosyal medya insanların kültürel, ekonomik ve sosyal hayatını etkilemiş ve herkesin hayatının vazgeçilmez bir parçası haline gelmiştir. Sosyal medya, kullanıcıların bir web sitesi veya uygulama ortamı aracılığıyla metin, ses, video, resim, grafik ve animasyon gibi multimedya içeriğine katılmasını ve paylaşmasını sağlayan bir platformdur (Soomro ve Hüseyin, 2019: 9). We Are Social ve Hootsuite ortaklığında yayınlanan yeni "Dijital 2022 Küresel Genel Bakış Raporu"na göre Dünyada 4,62 milyar sosyal medya kullanıcısı bulunmaktadır. Sosyal medya kullanıcılarının nüfusa oranı ülkemizde % 80'dir (recrodigital, 2022). Sosyal medya, birbirleriyle ilişkiler, karşılıklı çıkarlar ve bilgi alışverişi ile birbirine bağlı olan bireylerden oluşan bir ağ olarak tanımlanabilir. İnternet kullanımının artmasıyla birlikte insanlar sevdikleriyle iletişim kurmak için çoğunlukla sosyal paylaşım sitelerini tercih etmektedir (Maitlo vd., 2021: 2421).

Sosyal medya sitelerinin popülaritesini göz önünde bulundurarak, her türden kullanıcı, arkadaşları ve aileleriyle tanışmak, günlük rutinlerini sevdikleriyle paylaşmak ve yeni tanıdıklar bulmak için sosyal medya sitelerini kullanmaktadır. Sosyal medya siteleri, hayatın her kesiminden kullanıcıları kendine çekmektedir **(**Miquel vd., 2020: 124).

Dijilopedia'nın Ocak 2023 itibarıyla sosyal medya kullanıcılarına ilişkin verilerine göre dünyanın "favori" sosyal medya platformlarında Facebook hala ilk sıradadır. Instagram dördüncü sırada olmasına rağmen küresel internet kullanıcılarının yüzde 14,8'i Instagram'ı favori platformları olarak tanımlarken, bu oran Facebook için yüzde 14,5'tur. YouTube, platformun izleyicisinin Facebook'tan neredeyse iki kat daha hızlı büyümesiyle, geçen yıl Facebook ile arasındaki farkı kapatmıştır. YouTube'un şu anda en az 2,56 milyar aktif kullanıcısı bulunmaktadır. Bu durum en son Facebook kullanıcı toplamının kabaca yüzde 88'ine denk gelmektedir. Bununla birlikte, başka bir medya platformu olan WhatsApp internet kullanıcılarının yüzde 15,7'sinin en sevdikleri mesajlaşma uygulaması olarak seçilmiştir. Instagram, küresel düzeyde dördüncü sırada yer almaktadır (dijilopedia, 2023). Sosyal medyanın yaygın kullanımı bazı riskleri de beraberinde getirmektedir. Bu risklerin başında sosyal medyada işlenen suçlar gelmektedir.

Suç, kanunla yasaklanan fiil veya ihmalin eşlik ettiği ve sonuç olarak ihlali cezai yaptırımlar içeren herhangi bir davranıştır. Siber suç, siber dünyadaki en son ve belki de en karmaşık sorundur. "Siber suçun, türü konvansiyonel suç olan ve bilgisayarın suç oluşturan davranışın bir nesnesi veya öznesi olduğu türlerdir" (Dashora, 2011: 242). Siber suçun genelleştirilmiş tanımı, "bilgisayarın bir araç veya hedef veya her ikisi olduğu yasa dışı eylemler" olabilir. Pornografi, çevrimiçi kumar, fikri mülkiyet suçları, e-posta sahteciliği, sahtecilik, siber iftira, siber taciz bilgisayara/bilgisayar sistemine/bilgisayar ağlarına yetkisiz erişim, elektronik formda yer alan bilgilerin çalınması, veri dolandırıcılığı, bilgisayar sistemi hırsızlığı, bilgisayar sistemine fiziksel olarak zarar verme olarak sıralanabilir (Dashora, 2011: 243). Suç, şeklini gelenekselden elektroniğe doğru değiştirmektedir. Bir yandan sosyal medya kullanımı artarken, diğer yandan elektronik ortam suçları da artmaktadır. Suçlular suçu planlamak, yürütmek veya işlemek için gerçek zamanlı sosyal medyayı kullanmaktadır. Bununla birlikte kolluk kuvvetleri de sosyal medyayı suçu kontrol etmek, önlemek, korumak ve soruşturmak için kullanmaktadır (Soomro ve Hüseyin, 2019: 11). Siber suç, bilgisayar tabanlı sistemler kullanılarak siber uzayda gerçekleştirilen bir suç faaliyetidir. Kişisel bilgisayarlar, tabletler, akıllı telefonlar gibi bilgisayar tabanı sistemler suç işlemek için kullanılabileceği gibi mağduru olmak için de kullanılabilir. Siber suç, son zamanlarda sosyal medyanın artan kullanımı ile artmıştır (Arpacı ve Aslan, 2022: 1). Suç, bir toplumda yasalarca belirlenen kuralların ihlal edilmesidir (Zencirkıran, 2020: 245). Yasaların suç saydığı cezai yaptırımlara bağladığı, hukuka aykırı davranış olarak nitelendirilen suç kavramı ve yaptırımları ancak yasalar tarafından konulur veya kaldırılır bu nedenle bir eylem yasalar tarafından suç olarak tanımlanmamışsa hukuka aykırı bir hareket olsa bile suç olarak kabul edilmemektedir (Burkay, 2008: 3).

Suç, topluma, mekâna ve zamana göre farklı anlamlar barındırmaktadır. Herhangi bir zamanda veya herhangi bir yerdeki toplum tarafından suç olarak görülmeyen bir eylem farklı zamanda veya başka yerdeki toplum tarafından suç olarak kabul edilmektedir (Sandilaç, 2022: 152).

Bir gruba göre suç olarak görülen davranış başka bir gruba göre suç olmayabilir. Bu grubun içinde bulunduğu kültüre bağlıdır. Kültüre bağlı olarak nesiller boyu içeriği de farklılık göstermektedir (Çalış ve Karataş, 2020: 113). Suç dinamik bir yapıya sahiptir ve sürekli değişim göstermektedir. Örneğin teknolojinin gelişmesi ve bilgisayar sistemlerinin yaygınlaşması beraberinde bilgisayar ile suç işlemeyi getirmiş böylece bilgisayar suçları adı altında yeni bir suç türü ortaya çıkmıştır (Burkay, 2008: 4).

İnternette geleneksel suçların yanı sıra siber suçlar da görülmektedir. Bu, bir suçlu tarafından yeni suç biçimleri keşfedildiğinden ve elektronik iletişimi kullanan toplum tarafından daha az farkındalık olduğundan, erken dönemde bir suçlu için 'güvenli sığınaklara' yol açar. Sosyal medya, günümüzün topluluk iletişiminin yanı sıra her türlü internet tabanlı suç için bir ortamdır. Bu sosyal büyük veri, örneğin, tweet'ler, bloglar, SMS ve telefon görüşmeleri dahil olmak üzere sohbet mesajları, suçu önlemek için gerçek zamanlı olarak veya suçu araştırmak için çevrimdışı olarak kullanılabilir. Sosyal medya yalnızca topluluk için bir iletişim ortamı değil, aynı zamanda bu ortamdaki yanıt süresi çok hızlı olduğundan (gerçek zamanlı) suç topluluğu için de bir ortamdır. Şu anda sosyal medya, kolluk kuvvetlerinin suçu önleme aracı haline gelmiştir. Kolluk kuvvetleri, internet üzerinden iletişim faaliyetlerini izleyerek suçu önlemek için azami çabayı göstermektedir (Soomro ve Hüseyin, 2019: 10). Siber suç terimi, bilgisayarlar, dizüstü bilgisayarlar, tabletler, internet özellikli televizyonlar, oyun konsolları ve akıllı telefonlar aracılığıyla internet kullanılarak çevrimiçi olarak gerçekleştirilen çeşitli suçları ifade eder. Ayrıca teknoloji destekli suç, bilişim suçu, dijital suç, elektronik suç, sanal suç, net suç ve yüksek teknoloji suçu olarak da tanımlanmaktadır (Giri, 2020: 664).

Sosyal Medya ve Siber Suçlar

Sosyal medya aracılığıyla sosyal etkileşim hızla yüz yüze iletişimi geride bırakmaktadır. İnternetin günlük yaşamda artan yaygınlığıyla birlikte pek çok kişi Facebook, Twitter ve Instagram gibi sosyal medyadaki suçların mağduru olmuştur. Çevrimiçi suçlular, siber zorbalık, bilgisayar korsanlığı, kimlik hırsızlığı ve siber taciz gerçekleştirmek için bu siteleri hedefler (Miquel vd., 2020: 123).

Facebook, Twitter ve YouTube gibi sosyal medya sitelerinin milyonlarca aktif kullanıcısı vardır. Bu web sitelerini kullanarak insanlar birbirleriyle anında ve rahatlıkla iletişim kurarlar. Sosyal medya siteleri, insanlar tarafından birbirleriyle iletişim kurmak, kamu sektörü tarafından ise reklam ve yeni eleman alımı için kullanılmaktadır (Soomro ve Hüseyin, 2019: 11). Gerçekten de internet, siber zorbalık, siber kimliğe bürünme ve kimlik hırsızlığı gibi yeni suç faaliyetleri biçimlerinin önünü açmıştır. Bu faaliyetler internetin çeşitli işlevlerinde gerçekleşmekte ve Twitter, Instagram ve Facebook gibi sosyal medya siteleri muaf tutulmamaktadır (Miquel vd., 2020: 124). Sosyal medya ve siber suçlarla ilgili çeşitli literatür göz önüne alındığında, sosyal medya forumları, verilerin, kişisel bilgilerin, kişisel görüntülerin, mesajların, görüntülü görüşmelerin, düşüncelerin paylaşılmasını sağlayan en popüler iletişim araçları haline gelmiştir (Almadhoor vd., 2021: 2973).

Sosyal medyanın yaygınlaşması ve siber suçun artan yaygınlığı, özellikle çevrimiçi üniversite ortamlarında yüksek öğrenim ortamı için önemli zorluklar oluşturmaktadır. Sosyal medyanın iletişimi ve iş birliğini kolaylaştırmada sunduğu sayısız faydaya rağmen, öğrenciler arasında akademik performans ve ruh sağlığı üzerindeki olumsuz etkileri konusunda artan bir endişe bulunmaktadır. Ayrıca, siber zorbalık ve bilgisayar korsanlığı da dahil olmak üzere siber suçun artışı, çevrimiçi eğitim topluluğundaki bireylerin güvenliğini ve refahını tehdit etmektedir (Akrami vd., 2024: 23). Siber suç, bilgisayar cihazları ve teknoloji sistemleri kullanılarak işlenen çeşitli yasadışı eylemler için kullanılan bir terimdir (Bossler ve Berenblum, 2019: 495). Siber suçlar, bilgisayar sistemleri ve siber uzay bilgisi kullanılarak işlenir. Siber suçları işlemek için kullanılan cihazlar bilgisayarlarla sınırlı değildir, ayrıca tabletler, akıllı telefonlar, akıllı cihazlar ile de siber suçlar işlenmektedir (Umeugo, 2023: 25).

Siber suçlar, bir bireye veya bir grup kişiye karşı internet, e-posta, sohbet odaları veya sosyal medya gibi bilgisayar tabanlı teknolojileri kullanarak mali, hukuki, zihinsel, duygusal veya kasıtlı olarak zarar verme amacıyla işlenen suçlardır. Siber suçlar genellikle bir bireye karşı bilgisi olmadan işlenir; çünkü siber suçlular genellikle bu tür eylemlerin keşfedilmesini zorlaştırır. Siber zorbalık ve taciz, siber gasp, bilgisayar korsanlığı, telif hakkı ihlali, çevrimiçi aşk dolandırıcılığı, kimlik hırsızlığı ve çevrimiçi dolandırıcılık gibi birçok siber suç türü vardır. Siber zorbalık, bir birey veya bir grubun elektronik teknolojiyi kasten kullanarak rahatsız edici fotoğraflar, metinler, grafikler veya bu tür bilgileri başkalarına göndererek başkalarını tekrar tekrar taciz etmesi veya tehdit etmesidir (Miquel vd., 2020: 125).

Literatür, bilgisayarın suçla ilişkisine göre dört genel siber suç türünü sınıflandırmıştır (Jahankhani vd., 2017: 154):

a. Bilgi (örn. müşteri listesi, fiyatlandırma verileri veya pazarlama planı) ve bilgisayarlı dosyalardan elde edilen bilgilere (örn. tıbbi bilgiler, kişisel geçmiş veya cinsel tercih) dayalı şantaj.
b. Hedef Olarak Bilgisayar: Fikri mülkiyet hırsızlığı, pazarlama hırsızlığı.
c. Suç Aracı Olarak Bilgisayar: Otomatik para çekme makinesi (ATM) kartlarının ve hesaplarının hileli kullanımı, tahakkuk, dönüştürme veya transfer hesaplarından para çalınması, kredi kartı dolandırıcılığı, bilgisayar işlemlerinden (hisse senedi transferi, satış veya faturalama, dolandırıcılık) ve telekomünikasyon dolandırıcılığı.
d. Bilgisayar Diğer Suçlarla Tesadüftür: Kara para aklama ve yasa dışı bankacılık işlemleri, organize suç kayıtları veya defterleri ve bahisçilik.
e. Bilgisayarların Yaygınlığıyla İlişkili Suçlar: Yazılım korsanlığı/sahtecilik, bilgisayar programlarının telif hakkı ihlali, sahte ekipman, karaborsa bilgisayar ekipmanı ve programları ve teknolojik ekipman hırsızlığı.

Sosyal medya sadece bir iletişim aracı değil, aynı zamanda bu ortamdaki etki tepki süresinin hızlı olmasından dolayı suç dünyası için de önemli araç hâline gelmiştir. Diğer taraftan, sosyal medya, kolluk kuvvetlerinin suçu önlemesi içinde başvurulan araçtır. Facebook, Twitter ve YouTube gibi sosyal medya sitelerinin milyonlarca aktif kullanıcısı vardır ve bu web sitelerini kullanarak insanlar birbirleriyle anında iletişim sağlamaktırlar. Ulusal Beyaz Yaka Suçları Merkezi'nin "Sosyal Medyanın Suçlu Kullanımı" raporuna göre sosyal medya bağlamında; sosyal

medya üzerinden hırsızlık, sosyal medyada sahtekârlık ve kimlik avı, kötü amaçlı yazılım, kimlik hırsızlığı, siber taciz, siber yer tespiti olmak üzere altı suç türü bulunmaktadır (Cengiz, 2021: 415).

Sosyal Medyada Siber Suç Türleri

Bilişim teknolojileri yeni suç türlerinin ortaya çıkmasının yanı sıra var olan suçların daha kolay işlenmesine neden olmuştur (Kolukırık ve Gün, 2020: 324). Bilişim teknolojilerinin yaygın kullanım alanı olan sosyal medyada ortaya çıkan suç türleri de bireyler ve kurumlar açısından ciddi güvenlik zafiyetine yol açmaktadır.

Sosyal medyada suç türleri tablo 1 de gösterilmiştir.

Tablo 1. Sosyal Medyada Suç Türleri

Siber Suç	Önleme ipuçları	Önleme teknikleri
Sosyal medya aracılığıyla hırsızlık	Konum paylaşmayın Ev adresini paylaşmayın Kişisel bilgileri arkadaşlarınızın arkadaşlarıyla paylaşmayın Bağlantınızı yalnızca tanıdığınız kişilerle sınırlayın Gizlilik ayarınızı kontrol edin ve başkalarının sizi nasıl etiketleyebileceğini kontrol edin Uygulama izinlerinizi sınırlayın	Güvenlik kameraları, kapı kilitleri, monitörlü kör noktalar, hareketle Etkinleştirilen projektörler ve/veya rastgele zamanlayıcılı iç mekân lambaları vb. gibi gerekli fiziksel güvenlik tekniklerini kullanın
Sosyal Sahtekarlık ve E-dolandırıcılık	Bir web sitesinin güvenliğini kontrol etmeden önce hassas bilgileri internet üzerinden göndermeyin Kişisel veya mali bilgiler için istenmeyen aramalara, e-postalara veya ziyaretlere yanıt vermeyin Doğrudan şirketle iletişime geçerek şüpheli bir e-postanın meşruiyetini doğrulayın	Tek seferlik şifre (OTP) CAPTCHA Dijital sertifikalar Genetik ve nitelik tabanlı kimlik avı önleme algoritmaları Teknikler: Sinir ağı
Kötü amaçlı yazılım	Güncellenmiş antivirüs yükleyin Kullanıcının dikkatli olması gerekir Bir web sitesinin tek tip kaynak bulucusuna (URL) dikkat edin. Kötü amaçlı web siteleri meşru bir siteyle aynı görünebilir	İmza tabanlı kötü amaçlı yazılım tespiti. Anomali tabanlı kötü amaçlı yazılım tespiti. Teknikler:N-gramlar, API/sistem çağrıları, montaj talimatları ve hibrit özellikler
Kimlik Hırsızı	Sahibi, süresi dolmuş ehliyet gibi (süresi dolmuş) kimlik belgelerini imha etmelidir. Sosyal medyada, örneğin biniş kartı vb. kimlik belgelerinin paylaşılmasını kısıtlayın. Kredi kartı vb. kimlik belgelerini sistemde bulundurmayın/saklamayın	Üç faktörlü kimlik doğrulama (3FA) Biyometri Symantec'ten Life Lock gibi kimlik hırsızlığı önleme yazılımı Teknikler: SD ve CD algoritmaları
Siber Takip	İş ve sosyal ağ e-posta adreslerini ayrı tutun. Doğum tarihi veya	Mümkün olduğu kadar çok kanıt toplayın ve belgeleyin Siber

	çalışma geçmişi gibi tüm bilgileri çevrimiçi olarak koymayın Konumu tanımlamayan fotoğraflar kullanın. Sosyal medyada yasal isim kullanmayın; takma ad kullan Facebook, Twitter ve diğerleri gibi çeşitli platformlarda bulunan gizlilik ayarlarından yararlanın	takipçilere karşı bloke edin ve yetkililere bildirin Teknikler: birliktelik kuralı madenciliği, metin madenciliği, siber takip algılama çerçevesi ve imza tabanlı veri madenciliği
Siber Muhafaza	Akıllı telefonda GPS'inizi kapatın Siz dönene kadar tatil durumunu veya fotoğrafları herkese açık olarak yayınlamayın Çevrimiçi pazar yerlerinde ürün satarken evde müsait olacağınız zamanlardan bahsetmeyin	Bir görüntünün coğrafi konum içerip içermediğini kontrol etmek ve kaldırmak için tool.geoimgr.com gibi çevrimiçi araçları kullanın.
Kredi Kartı Dolandırıcılığı	Kasaların sürekli gözetimi Düzenli ve ciddi malzeme muhasebesi İmzalamak için kritik malzemeye dokunan çalışan günlüğü Kritik mülke erişmek için iki kişi kuralı uygulayın Çalış anın dikkatini güvenliğe teşvik edin	Anormallikleri izleme Teknikler: adres doğrulama hizmeti (AVS), kart doğrulama değeri (CVV), karar ağ acı, sinir ağ ı, k-ortalama kümeleme,
Siber Saldırı ve Veri İhlalleri	Son kullanıcı bilinçlendirme kampanyası tasarlayın ve yürütün Bilgisayar güvenlik ilkesini oluş turun ve uygulayın Verileri yalnızca ihtiyacınız olduğu sürece saklayın Bir olay müdahale planı hazırlayın İzinsiz giriş tespit ve önleme sistemini devreye alın Rutin güvenlik açığı değerlendirmesi yapın Tüm oturum açma kimlik bilgilerinin süresinin dolmadığından emin olun	Doğ ulama ve onaylama Kişisel kimlik numarası (PIN) veri tabanı (CVE), ortak zayıflık sıralama veri tabanı

Kaynak: (Soomro ve Hüseyin, 2019: 14-15).

a. Sosyal Medyada Hırsızlık

Sosyal medya yoluyla hırsızlık yapan suçlular, sosyal medyada hırsızlık için potansiyel bir hedef ararlar. Sosyal medya kullanıcıları genellikle kişisel aktivitelerini yayınlarlar. Suçlular, mülkü soymak için geniş bir zaman çerçevesi buldukları kolay hedefler bulmak için bu tür bilgileri ararlar. BBC'nin haberine göre, geçen yıl Kim Kardashian'a ait 10 milyon dolarlık mücevherin çalınması bu tür suçların en belirgin örneğidir (Soomro ve Hüseyin, 2019: 11). Suçlular potansiyel hırsızlık hedefleri için sosyal medyaya yönelmektedir. Sosyal medya kullanıcıları genellikle yenilen akşam yemeği veya gidilen tatil yerleri gibi kişisel aktivitelerini takipçileri ile paylaşmaktadırlar. Bu paylaşımlar hırsızları hareket geçirmekte ve hedeflerine yönelmeyi kolaylaştırmaktır (Cengiz, 2021: 416).

b. Sosyal Sahtekarlık ve Kimlik Avı

Müşterileri kandırarak kişisel güvenlik bilgilerini ifşa etme girişimidir; kredi kartı numaralarını, banka hesap bilgilerini veya diğer hassas bilgilerini bir e-postada güvenilir işletmeler gibi göstererek ifşa ederler. Mesajları, alıcılardan hesap bilgilerini "güncellemelerini", "doğrulamalarını" veya "onaylamalarını" isteyebilir. Birinci adımda, bilgisayar korsanı bir kuruluşun kimliğini çalar ve benzer bir web sitesi oluşturur. Bu, hedeflenen sitenin kaynak kodunu görüntüleyerek ve ardından o gerçek web sitesinden tüm grafikleri ve HTML satırlarını kopyalayarak kolayca yapılabilir. Bu taktik nedeniyle, deneyimli bir kullanıcının bile farklılıkları fark etmesi gerçekten çok zor olacaktır. Mimik web sitesinde, genellikle kullanıcıdan gizli kişisel verileri girmesini isteyen bir oturum açma formu olacaktır. Veriler buraya girildikten sonra, sunucu taraflı bir komut dosyası gönderimi işleyecek, verileri toplayacak ve bilgisayar korsanına gönderecek, ardından kullanıcıları gerçek web sitesine yönlendirerek her şeyin şüpheli görünmesini sağlayacaktır. Kimlik avı (sahtekarlık olarak da adlandırılır) terimi, İnternet dolandırıcılarının, kullanıcının finansal bilgilerini ve parola verilerini "avlarken" giderek daha karmaşık yemler kullanmalarından kaynaklanmaktadır (Jahankhani vd., 2017: 156).

Sosyal sahtekarlık, kişisel bilgileri elde etmek için psikolojik manipülasyon kullanır. Sosyal ağ sitelerini kullanan kişiler, arkadaşlarından acil mali yardım talep eden mesajlar alırlar. Aslında bu mesajlar arkadaşları tarafından değil, arkadaşlarının e-postalarını ve şifrelerini çalan suçlu tarafından gönderilmiştir. Doğasındaki kolaylığı nedeniyle, bilgisayar güvenlik firması Trend Micro, Facebook'u "dolandırıcılık mayın tarlası" olarak adlandırıyor. 2019/24 Huzurlu bir toplum ve huzurlu bir dünya her ülkenin, her insanın ve her araştırmacının hayalidir ama toplum varsa suç işleme olasılığı da vardır. Suç, şeklini gelenekselden elektroniğe doğru değiştiriyor. Bir yandan sosyal medya kullanımı artarken, diğer yandan elektronik ortam suçları da artıyor. Suçlular suçu planlamak, yürütmek veya işlemek için bu hızlı yanıt gerçek zamanlı sosyal medyayı kullanıyor ve kolluk kuvvetleri aynı sosyal medyayı suçu kontrol etmek, önlemek, korumak ve soruşturmak için kullanıyor. Siber suçlular, sosyal mühendislik hileleri ve taktikleri ile potansiyel hedef bilgilerini elde etmek için çeşitli yöntemlerden yararlanır. Kimlik avı e-postaları, çalışanlardan oturum açma kimlik bilgilerini isteyen patrondan veya kişinin bankasından gelmiş gibi görünebilir. Siber suçlular, rasyonel düşünmek yerine talimat verildiği gibi yapmak için hedeflerini korkutmayı garanti eder. Bu tekniği kullanan suçlu, yararlı bilgiler alma umuduyla milyonlarca e-posta gönderir. Kimlik avının en yaygın biçimi, Facebook veya Banka benzeri bir sayfa oluşturmaktır (Soomro ve Hüseyin, 2019: 11).

c. Kötü Amaçlı Yazılım

Sosyal medya, virüsleri ve kötü amaçlı yazılımları yaymak için harika bir platform sağlar. Reklam yazılımı, kötü amaçlı yazılım ve virüs geliştiricileri, yıkıcı programlarını herhangi bir sosyal ağ web sitesinde normal bir görev olan bağlantılarda, eklerde ve mesajlarda gizler. Kullanıcılar yanıt verdiğinde, kötü amaçlı yazılım onların bilgisi olmadan bilgisayarlarına bulaşır. Sophos antivirüs geliştiricisine göre, sosyal medya aracılığıyla kötü amaçlı yazılım kurbanları, kullanıcılarının %40'ını oluşturmaktadır. Microsoft, 19 milyon PC'ye haydut bir virüs bulaştığını bildirdi. Ayrıca iş dünyası, çalışanları tarafından sosyal medya kullanımını bir ağ güvenliği riski olarak görmektedir (Soomro ve Hüseyin, 2019: 12).

d. Kimlik Hırsızlığı

Kimlik hırsızlığı, suç faaliyeti için bir bireyin kişisel bilgilerini alma girişimi olarak tanımlamaktadır. Kimlik hırsızlığını, kurbanın kişisel bilgilerinin herhangi bir yasal yetki olmadan, suç işleme niyetiyle kasıtlı olarak kullanılması olarak algılamaktadır. FBI'ın İnternet Suçları Şikâyet Merkezi'nin (IC3) İnternet Suçları Raporu 2016'ya göre, kimlik hırsızlığı 16.878 kurbanla yedinci sırada yer aldı ve sadece ABD'de 58.917.398 USD kayıp kaydedildi (Soomro ve Hüseyin, 2019: 12).

Kimlik hırsızlığı, başka bir kişi hakkında onun bilgisi dışında hassas bilgiler edinme ve bu bilgileri hırsızlık veya dolandırıcılık yapmak için kullanma eylemidir. İnternet, siber suçlulara bu tür bilgileri savunmasız şirketlerin veri tabanından alma fırsatı verdi. Ayrıca mağdurları, hassas kişisel bilgileri meşru bir işletmeye ifşa ettiklerine inandırmalarına da olanak sağlamıştır; bazen fatura veya üyelik bilgilerinin güncellenmesini isteyen bir e-postaya yanıt olarak; bazen (sahte) bir İnternet iş ilanına başvuru şeklini alır. Tüm Parti Parlamento Grubuna göre hem Birleşik Krallık'ta hem de küresel olarak mevcut araştırmalar, kişisel bilgileri edinme ve kullanma yöntemlerinin

artması ve gelişmesi nedeniyle kimlik sahtekarlığının büyük ve büyüyen bir sorun olduğunu gösteriyor. Ardından, önümüzdeki yıllarda daha da artması bekleniyor (Jahankhani vd., 2017: 159).

e. Hacklemek

Bilgisayar korsanlığı, siber suç faaliyetinin en geniş çapta analiz edilen ve tartışılan biçimlerinden biridir ve bu tür faaliyetlerin toplum için oluşturduğu tehdide ilişkin kamu kaygıları için yoğun bir odak noktası görevi görür. Bilgisayar korsanlığının net tanımı, "diğer kişilerin bilgisayar sistemlerine yetkisiz erişim ve ardından kullanım"dır (Jahankhani vd., 2017: 157). Saldırılar, bilgi toplama veya keşif, tarama ve nihayet hedef sisteme girme gibi birkaç aşamada gerçekleşir. Bilgi toplama, bilgi edinme veya güvenlik açıkları açma yöntemlerini içerir. Tıpkı geleneksel soygun türünün gerçekleştirilme şekli gibi. Soyguncu, girişimde bulunmadan önce soymak istediği yerle ilgili tüm bilgileri öğrenecektir. Tıpkı bunun gibi, bilgisayar saldırganı hedef hakkında bilgi bulmaya çalışacaktır. Sosyal Mühendislik, bir saldırgan tarafından bilgi almak için kullanılan böyle bir yöntemdir (Jahankhani vd., 2017: 158).

f. Siber Taciz ve Zorbalık

Siber taciz veya zorbalık, e-posta, anlık mesajlaşma, kısa mesajlar, bloglar, cep telefonları, çağrı cihazları, anlık mesajlar ve iftira niteliğindeki web siteleri gibi elektronik bilgi ve iletişim araçlarının bir bireyi veya grubu kişisel yollarla zorbalık veya başka bir şekilde taciz etmek için kullanılmasıdır. "En azından fiziksel bir kavgada bir başlangıç ve bir son vardır, ancak alaylar ve aşağılamalar bir çocuğu evine kadar takip ettiğinde, bu bir 'işkencedir' ve bitmez" (Early, 2010). İnternet üzerinden veya cep telefonlarından gönderilen kısa mesajlar üzerinden siber zorbalık, alay etme, hakaret ve taciz, bazı durumlarda trajik sonuçlarla birlikte gençler arasında yaygın hale geldi (Jahankhani vd., 2017: 159).

Materyal ve Metot

Anket soruları hazırlanırken demografik özelliklere ilişkin sorular ile Arpacı ve Aslan tarafından geliştirilen "Sosyal Medyada Siber Suç Farkındalığı Ölçeği"nden kullanım izini alınmak suretiyle yararlanılmıştır (Arpacı ve Aslan, 2022: 1-11). Ana kütledeki veri sayısı N ve örneklem sayısı da n olmak üzere örneklem büyüklüğü hesaplanırken N (Erzincan Binali Yıldırım Üniversitesi Sosyal Hizmet Bölümü Öğrencileri) =612'dir. Örneklem sayısı (n)=346 kişi olur (Karagöz, 2019: 308). Yapılan çalışmada 0,05 anlamlılık düzeyinde basit tesadüfi örnekleme yoluyla seçilen 346 kişi örnekleme dahil edilmiştir. Sosyal medyada siber suç farkındalığı ölçeğinin güvenilirlik analizi ,955 çıktığından uygulanan anketin sonuçları oldukça güvenilirdir. Arpacı ve Aslan'ın (2022) çalışmalarında da ölçeğin Cronbach Alfa değeri .957'dir (Arpacı ve Aslan, 2022: 6).

Araştırmanın Hipotezleri ve Alt Hipotezleri: Üniversite öğrencilerinin sosyal medyada siber suç farkındalığı demografik özelliklerine göre farklılaşmaktadır.

H_1: Üniversite öğrencilerinin cinsiyeti ile sosyal medyada siber suç farkındalığı arasında bir fark vardır.

H_2: Üniversite öğrencilerinin sınıfı ile sosyal medyada siber suç farkındalığı arasında bir fark vardır.

H_3: Üniversite öğrencilerinin sosyal medyada geçirdikleri süre ile sosyal medyada siber suç farkındalığı arasında bir fark vardır

H_4: Üniversite öğrencilerinin sosyal medyayı kullanım amacı ile sosyal medyada siber suç farkındalığı arasında bir fark vardır.

Bulgular

Bu bölümde araştırma sonucunda ortaya çıkan sonuçlar açıklanmaktadır.

Güvenilirlik Analizi

Tablo 2. Sosyal Medyada Siber Suç Farkındalığı Ölçeğinin Güvenilirlik Analizi

Ölçek	İfade Sayısı	Cronbach's Alfa
Sosyal Medyada Siber Suç Farkındalığı Ölçeği	22	,955

Araştırma sonucumuzda Cronbach's Alpha değeri 0.95 çıkmıştır.

Katılımcıların Demografik Profili ve Betimsel İstatistikler

Tablo 2. Katılımcıların Demografik Özelliklerine İlişkin Tablo

Demografik Özellikler		**Kişi Sayısı**	**Yüzde**
Cinsiyet	Kadın	284	82,1
	Erkek	62	17,9
Sınıf	1.sınıf	90	26,0
	2.sınıf	98	19,1
	3.sınıf	66	8,2
	4.sınıf	92	26,6

Katılımcıların %82,1'i 284 kişi kadın, %17,9'u 62 kişi erkektir. Sınıf açısından değerlendirdiğimizde en çok katılımı %26,6'lık oranla 92 kişiyle 4.sınıf öğrencileri oluşturmaktadır. En az katılımı %8,2'lük oranla 66 kişiyle %8, 2 oranla 3. Sınıf öğrencileri oluşturmaktadır.

Tablo 3. Katılımcın Sosyal Medya Kullanımına İlişkin Sorular

Sosyal Medya Kullanımına İlişkin Sorular		**Kişi Sayısı**	**Yüzde**
Sosyal medya hesabınız var mı?	Evet	330	95,4
	Hayır	16	4,6
Sosyal medyaya hangi cihazı kullanarak katıyorsunuz?	Bilgisayar	6	1,7
	Cep telefonu	340	98,3
Hangi sosyal medya uygulamasını kullanıyorsunuz?	Twitter	26	7,5
	Youtube	14	4,4
	Instagram	204	59,0
	Tiktok	2	,6
	Pinterest	2	,6
	Whatsapp	82	23,7
	Snapchat	14	4,0
	Linkedln	2	,6
	4 saatten az	152	43,9

Ortalama günlük kaç saat sosyal medyada zaman geçiriyorsunuz?	4-5 saat	124	35,8
	6-7 saat	44	12,7
	7 saat ve üzeri	26	7,5
Sosyal medyayı kullanım amacınız	Arkadaşlarım ve ailemle iletişim kurmak	92	26,6
	Fotoğraf ve video paylaşmak	18	5,2
	Boş zaman değerlendirmek	172	49,7
	Video izlemek	16	7,5
	Alışveriş yapmak	2	,6
	Duygusal boşluk, sorun ve problemlerden kaçmak	36	10,4

Katılımcıların %95,4'ünün sosyal medya hesabı bulunmaktadır. Katılımcıların %98,3'ü cep telefonundan sosyal medya uygulamalarına katılmaktadır.

Ahmead ve arkadaşlarının 2024 yılında yapmış oldukları çalışmada Al Quds Üniversitesi'ndeki lisans öğrencilerinin % 91'i mobil cihazlardan internet erişimini sağlamaktadır (Ahmead vd., 2024: 16). En çok kullanılan sosyal medya uygulaması %59,0'lık oranla 204 kişi Instagram kullanmaktadır. En az kullanılan sosyal medya uygulamaları ise Tiktok, Pinterest ve Linkedln olmuştur. Ortalama günlük sosyal medyada kullanılan zamana baktığımızda katılımcıların %43,9'u 4 saatten az, %35,8'i 4-5 saat, %12,7'si 6-7 saat ve %7,5'u 7 saatten fazla sosyal medyada zaman geçirmektedirler.

Arpacı ve Aslan'ın (2022) çalışmalarında katılımcıların %86,6'sı öğrencilerden oluşmaktadır. Sınıf seviyeleri %42,9'u birinci sınıf, %23,3'ü ikinci sınıf, %9,5'i üçüncü sınıf, %7,9'u dördüncü sınıf öğrencisiydi. Katılımcıların %20,7'si sosyal medyayı günde 1-2 saat, %42,8'i sosyal medyayı 3-4saat, %24,8'i sosyal medyayı 5-6 saat, %6,4'ü sosyal medyayı 7-8 saat kullanmaktadır (Arpacı ve Aslan, 2022: 5). Katılımcılar Youtube, Twitter, Instagram ve Whatsapp en çok kullanılan sosyal medya uygulamalarıdır (Arpacı ve Aslan, 2022: 6).

Hamzah ve arkadaşlarının 2021 yılında Malezya'da yapmış oldukları çalışmada sosyal tüm katılımcıların kendi sosyal medya hesapları olduğu ve kullanılan en popüler sosyal medyalar Instagram, Youtube, Facebook ve Twitter olduğu sonucuna ulaşmışlardır. Çoğu katılımcı günde 3-6 saatini (%32) sosyal medyayı kullanmaktadır (Hamzah vd., 2021: 696).

Katılımcıların sosyal medyayı kullanım amacına baktığımızda ise; katılımcıların %49,7'si 172 kişi sosyal medyayı boş zaman değerlendirmek için kullanmaktadır. %26,6'sı arkadaşları ve ailesiyle iletişim kurmak için kullanmaktadır. Alışveriş yapmak amacıyla sosyal medyayı kullananların sayısı ,6 oranla en düşüktür.

Tablo 4. Sosyal Medyada Siber Suç Farkındalığı Ölçeği Normallik Testi

Descriptives		
	Statistic	Std. Error

sosyalmedyadasibersuçfarkındalığıölçeği	Mean		1,3016	,02220
	95% Confidence Interval for Mean	Lower Bound	1,2580	
		Upper Bound	1,3453	
	5% Trimmed Mean		1,2569	
	Median		1,0909	
	Variance		,171	
	Std. Deviation		,41293	
	Minimum		1,00	
	Maximum		2,91	
	Range		1,91	
	Interquartile Range		,55	
	Skewness		1,510	,131
	Kurtosis		1,700	,261

Tabachnick and Fidell, (2013)' e göre normal dağılım testinde Skewness ve Kurtosis değerlerinin +1,5 ile -1,5 arasında ise veriler normal dağılıma uygundur. Sosyal Medyada Siber Suç Farkındalığı Ölçeği'nin normallik testi sonucunda ölçeğin minimum değeri 1,00 maksimum değeri 2,91'dir. Ölçeğin Skewness değeri 1,510 ve Kurtosis değeri 1,700'dür. Veriler normal dağılıma uygun olmadığından nanparametrik hipotez testleri kullanılacaktır. Veriler normal dağılıma uygun olmadığından nanparametrik hipotez testleri başlığı altında Kruskal-Wallis ve Mann-Whitney U testleri kullanılacaktır.

Cinsiyet Değişkenine Göre Sosyal Medyada Siber Suç Farkındalığı Düzeyi

Tablo 5. Cinsiyet Değişkenine Göre Sosyal Medyada Siber Suç Farkındalığı

Bağımsız Değişen	**N**	**Sıra Ortalaması**	**U**	**P**
Kadın	284	171,96	8366,000	,529
Erkek	62	180,56		

Katılımcıların cinsiyete göre sosyal medyada siber suç farkındalığı arasında %5 anlamlılık düzeyinde istatistiksel olarak anlamlı bir fark bulunmamıştır (P = 0,529 < = α 0,05). Diğer bir ifadeyle H_1 hipotezi reddedilmiştir.

Sınıf Değişkenine Göre Sosyal Medyada Siber Suç Farkındalığı Düzeyi

Tablo 6. Sınıf Değişkenine Göre Sosyal Medyada Siber Suç Farkındalığı

Bağımsız Değişen	**N**	**Sıra Ortalaması**	**χ2**	**sd**	**p**
1.sınıf	90	181,08	3,340	3	,342
2.sınıf	98	176,91			

3.sınıf	66	179,98			
4.sınıf	92	157,80			

Katılımcıların sınıfına göre sosyal medyada siber suç farkındalığı arasında %5 anlamlılık düzeyinde istatistiksel olarak anlamlı bir fark bulunmamıştır (P = 0,342 < = α 0,05). Diğer bir ifadeyle H_2 hipotezi reddedilmiştir.

Sosyal Medyada Geçirilen Süre Değişkenine Göre Sosyal Medyada Siber Suç Farkındalığı Düzeyi

Tablo 7. Sosyal Medyada Geçirilen Süre Değişkenine Göre Sosyal Medyada Siber Suç Farkındalığı

Bağımsız Değişen	**N**	**Sıra Ortalaması**	**χ2**	**sd**	**p**
4 saatten az	152	180,82	1,930	3	,587
4-5 saat	124	167,42			
6-7 saat	44	174,05			
7 saat ve üzeri	16	158,81			

Sosyal medyada geçirdikleri süre ile öğrencilerinin sosyal medyada siber suç farkındalığı arasında %5 anlamlılık düzeyinde istatistiksel olarak anlamlı bir fark bulunamamıştır (P = 0,587 < = α 0,05). Diğer bir ifadeyle H_3 hipotezi reddedilmiştir.

Sosyal Medyada Kullanım Amacı Değişkenine Göre Sosyal Medyada Siber Suç Farkındalığı Düzeyi

Tablo 8. Sosyal Medyada Kullanım Amacı Değişkenine Göre Sosyal Medyada Siber Suç Farkındalığı

Bağımsız Değişen	**N**	**Sıra Ortalaması**	**χ2**	**sd**	**p**
Arkadaşlarım ve ailemle iletişim kurmak	92	170,48			
Fotoğraf ve video paylaşmak	18	234,72	10,018	5	0,75
Boş zaman değerlendirmek	172	169,59			
Video izlemek	26	174,65			
Alış veriş yapmak	2	63,50			
Duygusal boşluk, sorun ve problemlerden kaçmak	36	174,56			

Katılımcıların sosyal medyayı kullanım amacı değişkeni açısından değerlendirildiğinde, katılımcıların sosyal medyayı kullanım amacı ile öğrencilerinin sosyal medyada siber suç farkındalığı arasında %5 anlamlılık düzeyinde istatistiksel olarak anlamlı bir fark bulunmuştur (P =0,075 < = α 0,05). Yani H_4 hipotezi kabul edilmiştir.

Sonuç

Gelişen bilgi iletişim teknolojileri ve internetle birlikte insanların iletişim kurma ve ihtiyaçlarını karşılama alanları da değişime uğramıştır. Sosyal medyanın bugün insanların hayatında önem bir yer tuttuğu bilinmektedir. Boş zaman faaliyetlerinin değerlendirilmesi, iletişim ve etkileşim kurmanın yanında resim ve video paylaşımı gibi birçok uygulamaya sahip olan sosyal medya insanlar için bazı risk ve tehlikeleri de beraberinde getirmektedir. Dijital bir kimlik ya da kullanıcı adıyla bir şifre aracılığıyla girilen sosyal medya uygulamaları kullanıcılarının çeşitli suç gruplarının hedefi haline gelmesine yol açmaktadır. Geleneksel anlamda suçun ortaya çıkışı, işlenen suçun türleri ve sonuçları sosyal medya alanına da taşınmıştır. Bu anlamda sosyal medyayı en çok kullanan kesim olarak üniversite öğrencilerinin sosyal medyada işlenen siber suçlar hakkında bilgi düzeyinin ve farkındalığının olup olmadığı amacıyla bu makale çalışması yapılmıştır. Araştırmada, üniversite öğrencilerinin sosyal medyada siber suçlara yönelik bilgi sahibi olup olmadıklarını belirlemek amacıyla hazırlanan anket soruları öğrencilere uygulanmıştır. Anket yoluyla elde edilen verilen SPSS programında analiz edilmiştir.

Araştırma sonucunda, öğrencilerin sosyal medyadaki siber suçlar konusundaki bilgilerine yönelik farkındalık düzeylerinin yüksek düzeyde olduğu tespit edilmiştir. Araştırma sonucunda araştırmaya katılan öğrencilerin %95 inin sosyal medya hesabı olduğu sosyal medyaya %98 oranında cep telefonlarından katıldıkları belirlenmiştir. Öğrencilerin en çok kullandıkları sosyal medya hesabı Instagram'dır. Bu sonuçlar 2023 dijilopedia sonuçlarıyla benzerlik göstermektedir. Veriler normal dağılmadığı için nanparametrik testler yapılmıştır. Bu testler neticesinde; H_1, H_2 ve H_3 hipotezlerimiz reddedilirken H_4 hipotezimiz kabul edilmiştir. Üniversite öğrencileri siber suç konusunda bilgi sahibi oldukları gibi sosyal medyanın kullanım amacına bağlı olarak siber suçların ortaya çıkabileceği konusunda bilgi sahibidirler. Bu çalışma, üniversite öğrencileri arasında siber suç riskleri farkındalık düzeyini, internete yönelik tutum gerçekliğini ve bunlar arasındaki ilişkiyi belirlemeyi amaçlamaktadır. Bu nedenle öncelikle siber suçlara karşı en savunmasız gruplardan biri olan üniversite öğrencilerine odaklanmıştır. Öğrencilerin siber suçlar konusunda daha olgun ve bilinçli oldukları ve şüpheli web sitelerini veya bağlantıları takip etmekten veya bunlarla etkileşime girmekten kaçınmak için yeterli bilgiye sahip oldukları sonucuna varılmıştır. Siber suçun ortaya çıkışı ve etkileri konusunda araştırmaya konu olan üniversite öğrencileri arasında her zaman siber suçlarla mücadele etme zorunluluğu olacaktır. Ancak bunu yalnızca bireylerin ve siber suçlarla mücadele konusunda ilgili kurumların ortaklığı ve iş birliğiyle başarılı bir şekilde yapılabilir. Güvenli, emniyetli ve güvenilir bir bilgi işlem ortamı sağlamak için etkili mücadele yöntemi geliştirilmelidir. Sonuç olarak, bu çalışmadan elde edilen bulgular, sosyal medyanın ve siber suçun yüksek öğrenimdeki olumsuz etkilerinin daha derin bir şekilde anlaşılmasına katkıda bulunmaktadır. Öğrencilerin algılarını ve davranışlarını inceleyerek ve bu zorlukları ele almak için etkili önlemleri belirleyerek, bu araştırma çevrimiçi yüksek öğrenim ortamlarındaki eğitimciler, politikacılar ve paydaşlar için değerli öngörüler sunmaktadır.

Çıkar Çatışması Beyanı

Yazar, bu makalenin araştırma, yazarlık ve/veya yayın süreci ile ilgili herhangi bir potansiyel çıkar çatışması olmadığını beyan eder.

Mali Destek

Yazar bu makalenin araştırılması, yazılması ve/veya yayınlanması için herhangi bir mali destek almamıştır.

Yayın Etiği Beyanı

Çalışmada etik dışı bir husus bulunmadığını, araştırma ve yayın etiğine özenle uyulduğunu beyan ederiz.

Yazar Katkı Oranı

Çalışma, yazar tarafından yürütülmüş ve raporlanmıştır.

Etik Kurul İzni

"Sosyal medyada siber suçlar: Üniversite gençliği üzerine uygulama" adlı bu çalışma için ERZİNCAN BİNALİ YILDIRIM ÜNİVERSİTESİ İNSAN ARAŞTIRMALARI SOSYAL VE BEŞERİ BİLİMLER, Bilimsel Araştırma ve Yayın Etiği Kurulu'ndan 25/12/2024 tarih ve 11/5 sayılı kararı ile etik kurul onayı alınmıştır.

Kaynakça

Ahmead, M., El Sharif, N. & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. *Crime Science,* 13(29), 1-19.

Akrami, K., Akrami, M., Ahrari, Hakimi, M. & Fazil, A.W. (2024). Investigating the adverse effects of social media and cybercrime in higher education: a case study of an online university, studies in media. *Journalism and Communications*, 2(1), 20-34.

Almadhoor, L., Alserhani, F. & Humayun, M. (2021). Social media and cybercrimes. *Turkish Journal of Computer and Mathematics Education,* 12(10), 2972-2981.

Arpaci, I., & Aslan, O. (2022). Development of a scale to measure cybercrime-awareness on social media. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2022.2101160.

Bossler, A.M. & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice,* 42(5), 495–499.

Burkay, S. (2008). Teorik çerçevede suç. *Felsefe ve Toplumsal Bilimlerde Diyaloglar*, 2(4), 2-3.

Büyüköztürk, Ş. (2010). *Sosyal bilimler için veri analizi el kitabı: İstatistik Araştırma Deseni SPSS Uygulamaları ve Yorum,* Ankara: Pegem Akademi Yayınları.

Cengiz, G. (2021). Siber suçlar, sosyal medya ve siber etik. *İletişim Çalışmaları Dergisi,* 7(3), 407-424.

Çalış, N. & Karataş, Z. (2020). Kavramsal ve güncel boyutlarıyla sosyal sorunlar. (Ed. Nurullah Çalış ve Zeki Karataş), İstanbul: Efe Akademi.

Dashora, K. (2011). Cyber crime in the society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences*, 3(1), 240-259.

George, D., & Mallery, M. (2010). *SPSS for Windows step by Step: A simple quide and reference, 17.0 update (10a ed.)* Boston: Pearson.

Giri, S. (2020). Cyber crime, cyber threat, Cyber Security Strategies and Cyber Law in Nepal. *Pramana Research Journal,* 9(3), 662-674.

Hamzaha , S., Fauziah, A. & Ramelic, N. (2021). Level of awareness of social media users on cyber security: case study among students of university tun hussein onn malaysia. *Turkish journal of computer and mathematics education*, 12(2), 694- 698.

Jahankhani, H., Al-Nemrat, A. & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics *in Cyber Crime and Cyber Terrorism Investigator's Handbook*, Amsterdam, The Netherlands:Elsevier, sh.149-166.

Karagöz, Y. (2019). *SPSS AMOS META Uygulamalı İstatistiksel Analizler*. Nobel Yayınları, Ankara.

Kaur, G., Bonde, U., Pise, K. L., Yewale, S., Agrawal, P., Shobhane, P., Maheshwari, S., Pinjarkar, L., & Gangarde, R. (2024). Social media in the digital age: a comprehensive review of ımpacts, challenges and cybercrime. *Engineering Proceedings*, 62(1), 1-12.

Kolukırık, S., & Gün, E. (2020). Bilişim teknolojilerinin suç eylemi üzerindeki etkisi: internet haberlerinde dijital suç örneği. *Journal of World of Turks/Zeitschrift für die Welt der Türken*, 12(3), 8-10.

Maitlo, A., Shoro, S., Nawaz, Haque & Soomro, I. (2021). Cyber attacks ımpacting on communication using social media: systematic review using data cluster ball. *International journal of advanced trends in computer science and engineering*, 10(3), 2421 – 2429.

Miguel, C.S., Morales, K. & Ynalvez, M.A. (2020). Online victimization, social media utilization, and cyber crime prevention measures. *Asia-pacific social science review* 20(4), 2020, pp. 123–135.

Mwiraria, D., Ngetich, K., & Mwaeke, P. (2024). Exploring Individual Factors Associated with the Prevalence of Cybercrime Victimization Among Students at Egerton University, Kenya. *European Journal of Humanities and Social Sciences,* 4(5), 35–40.

Sandilaç, N. (2022). Siber suç, siber terör ve siber savaş üçgeninde siber dünya. Bilişim Hukuk Dergisi, 4(1), 81-140.

Tabachnick, B. G., & Fidell, L. S. (2013). *Using Multivariate Statistics (6th ed.)*. Boston, MA: Pearson.

Umeugo, W. (2023). Cybercrime awareness on social media: A comparison study. *International Journal of Network Security & Its Applications*, 15(2), 23-35.

https://recrodigital.com/dunyada-ve-turkiyede-internet-sosyal-medya-kullanimi-2022/

EXTENDED SUMMARY

In the developing technological age, the internet, especially social media, plays an important role in our lives. Because thanks to social media, everyone can easily communicate with their relatives and loved ones. Its use is increasing day by day, which makes it easier for cybercriminals to carry out cyber activities using these networks. There are many networks such as Instagram, Twitter, Facebook, Youtube and Linkedin that users use daily, but can easily communicate with their families, friends and relatives and share their data. Social media has opened up new ways of communication in the internet-connected world. This communication includes sharing tweets, photos, pictures, likes and comments, etc. between people all over the world. In the past few years, online social networking sites have played an important role for users to communicate with their families, friends, professional groups and other communities using social media such as Twitter, Facebook, LinkedIn, MySpace, YouTube, Tiktok, WhatsApp. However, social media sites pose various serious security risks and threats to users. This article investigates whether the students of Erzincan Binali Yıldırım University, Faculty of Economics and Administrative Sciences, Department of Social Work are aware of the threats and security risks that may arise in terms of cybercrime on social media. As a result of the research, it was concluded that the students are aware of the cybercrimes that may occur on social media.

Social media has affected people's cultural, economic and social life and has become an indispensable part of everyone's life. Social media is a platform that allows users to participate and share multimedia content such as text, audio, video, images, graphics and animations through a website or application environment. According to the new "Digital 2022 Global Outlook Report" published in partnership with We Are Social and Hootsuite, there are 4.62 billion social media users in the world. The ratio of social media users to the population is 80% in our country (recrodigital, 2022). Social media can be defined as a network of individuals connected to each other through relationships, mutual interests and information exchange. With the increase in internet use, people mostly prefer social networking sites to communicate with their loved ones. Considering the popularity of social media sites, users of all types use social media sites to meet their friends and family, share their daily routines with their loved ones, and find new acquaintances. Social media sites attract users from all walks of life.

While preparing the survey form, questions about demographic participation and the "Cyber Crime Awareness Scale in Social Media" recorded by Arpacı and Aslan were used to obtain permission for use. When calculating the totals, where N is the data number in the main mass and n is their number, N (Erzincan Binali Yıldırım University Social Work Department students) = 612. The sample size (n) = 346 people . 346 people selected through simple random application at a significance level of 0.05 were included in the manual operation. When the publication analysis of social media cyber game performance is applied, 955 the results of the applied survey are quite reliable. The Cronbach Alpha value, which was also observed in the studies of Arpacı and Aslan (2022), is .957. With the developing information and communication technologies and the internet, the areas where people communicate and meet their needs have also changed. It is known that social media has an important place in people's lives today. In addition to evaluating leisure activities, communicating and interacting, social media, which has many applications such as sharing pictures and videos, also brings some risks and dangers for people. Social media applications, which are entered through a digital identity or username and a password, cause their users to become targets of various criminal groups. The emergence of crime in the traditional sense, the types of crimes committed and their consequences have been transferred to the social media area. In this sense, this article was conducted to determine whether university students, who use social media the most, have the level of knowledge and awareness about cybercrimes committed on social media. As a result of the research, it was determined that the students' awareness levels regarding their knowledge about cybercrimes on social media are high. As a result of the research, it was concluded that 95% of the students participating in the research have social media accounts and 98% of them participate in social media from their mobile phones. It was concluded that the most used social media account is Instagram. These results are similar to the 2023 dijilopedia results. Since the data was not normally distributed, nonparametric tests were performed. As a result of these tests; our H1, H2 and H3 hypotheses were rejected, while our H4 hypothesis was accepted. University students are knowledgeable about cybercrime, as well as the fact that cybercrimes can occur depending on the purpose of using social media. There will always be a need to combat cybercrime among undergraduate students who are the subject of research on the emergence and effects of cybercrime. However, we can only do this successfully with the partnership and cooperation of individuals and relevant institutions in combating

cybercrime. An effective combat method should be developed to provide a safe, secure and reliable computing environment.